UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/932,461	08/20/2001	Skye M. Poier	406.0005CIP	3781

25534 7590 12/21/2004

CAHN & SAMUELS LLP
2000 P STREET NW
SUITE 200
WASHINGTON, DC 20036

EXAMINER	
BATURAY, ALICIA	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/932,461	POIER ET AL.	
	Examiner	Art Unit	
	Alicia Baturay	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 January 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12082004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 are pending.

Drawings

2. The drawings are objected to because the label for the computer system (element 10), as described as appearing on Figure 1 in paragraph 31 of the specification, is not shown on Figure 1. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities: on page 19, paragraph 42, line 6, Applicant states "packet memorizing the external IP header..." It is believed Applicant meant to write "packet *memorizes* the external IP header..."Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 17 recites the limitation "said node" in the last line of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 4-6, 8, and 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Muniyappa et al. (U.S. 6,092,200).

8. As to claim 1, Applicant Admitted Prior Art (AAPA), Muniyappa, discloses a method for establishing a system for secure communications between nodes in a workgroup over a public network by facilitating the creation of a virtual private network (VPN), including a VPN server (Muniyappa, Fig. 1, element 20; col. 5, lines 5-7), the method comprising the steps of: establishing a secure connection between at least a pair of nodes within the workgroup and the VPN server (Muniyappa, col. 3, lines 33-38); and synchronizing each of the connected nodes with the VPN server such that each of the connected nodes receives configurational information relating to attributes of each of the other connected nodes (Muniyappa, col. 5, lines 25-39); where, when an attribute relating to one of the connected nodes or the VPN server is revised, the configurational information relating to the attribute is updated at each of the connected nodes (Muniyappa, col. 6, lines 18-29).

9. As to claim 2, Muniyappa discloses the invention substantially as described in claim 1, including the method for establishing the system further comprising, following the step of establishing the secure connection, a step of authorizing, at the VPN server, validity of the connection between the VPN server and each of the connected nodes (Muniyappa, col. 3, line 56 – col. 4, line 9).

10. As to claim 4, Muniyappa discloses the invention substantially as described in claim 1, including the method for establishing the system where the VPN server enables secure exchange of the configurational information between the connected nodes (Muniyappa, col. 5, lines 37-48).

11. As to claim 5, Muniyappa discloses the invention substantially as described in claim 1, including the method for establishing the system where the VPN server restricts exchanges of configurational information based on trust relationships established by the connected nodes (Muniyappa, col. 5, lines 36-50).

12. As to claim 6, Muniyappa discloses the invention substantially as described in claim 1, including the method for establishing the system where each of the connected nodes remains in a loop with the VPN server so as to forward any attribute revisions changes within a node to each of the connected nodes (Muniyappa, col. 6, lines 18-29).

13. As to claim 8, Muniyappa discloses a system for establishing secure communication between nodes in a workgroup over a public network by facilitating the creation of a virtual private network, the system comprising: at least a pair of nodes (Muniyappa, Fig. 1, elements 22 and 24); a VPN server (Muniyappa, Fig. 1, element 20), connected with each of the at least a pair of nodes for synchronizing each of the connected nodes with the VPN server such that each of the connected nodes receives configurational information relating to attributes of the other connected nodes or the VPN server (Muniyappa, col. 5, lines 25-39); where, when an

attribute relating to one of the connected nodes or the server is revised, the configurational information relating to the attribute is updated at each of the connected nodes (Muniyappa, col. 6, lines 18-29).

14. As to claim 10, Muniyappa discloses the invention substantially as described in claim 8, including where the system further comprises a client application located at each of the connected nodes (Muniyappa, col. 4, lines 17-24).

15. Claims 11-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Ylonen (U.S. 6,795,917).

16. As to claim 11, Ylonen discloses a method for establishing a system for secure transfer of a data packet between a first node and a second node in a workgroup over a public network, where the nodes are members of a virtual private network (Ylonen, col. 1, lines 23-26), the method comprising the steps of: assessing a presence of a device associated with the connected first and second nodes (Ylonen, Fig. 1, element 100); modifying a packet header of the data packet intended for transfer between the first and second nodes when a device is detected; where the modification of the packet headers facilitates traversing the detected device for transmission of the data packet between the first node and the second node (Ylonen, col. 1, lines 53-67).

17. As to claim 12, Ylonen discloses the invention substantially as described in claim 11, including the method for establishing the system where the modified packet header comprises an Encapsulated Security Payload (ESP) header (Ylonen, Fig. 5a, element 503), an Internet Protocol (IP) header (Ylonen, Fig. 5a, element 501), and a masquerade bit, the masquerade bit acting as an indicator to one of the first and second nodes that the data packet has been modified (Ylonen, col. 6, lines 33-35).

18. As to claim 13, Ylonen discloses the invention substantially as described in claim 12, including the method for establishing the system where the masquerade bit is located between the ESP header and the IP header (Ylonen, col. 6, lines 33-35).

19. As to claim 14, Ylonen discloses the invention substantially as described in claim 12, including the method for establishing the system where a packet interception mechanism analyses the packet headers for detecting the presence of the masquerade bit (Ylonen, col. 3, lines 40-47).

20. As to claim 15, Ylonen discloses the invention substantially as described in claim 13, including the method for establishing the system where when the masquerade bit is detected within the packet header, the modified packet header is removed and the original packet header of the data packet routes the data packet to one of the first and second node (Ylonen, col. 1, lines 53-67).

21. As to claim 16, Ylonen discloses the invention substantially as described in claim 11, including the method for establishing the system where the device is selected from a group comprising a Network Address Translation (NAT) Device, a firewall, a gateway, a proxy server, and combinations thereof (Ylonen, col. 1, lines 65-67).

22. As to claim 17, Ylonen discloses the invention substantially as described in claim 11, including the method for establishing the system where when a device is detected, the device is located in front of the node (Ylonen, Fig. 1, element 100).

23. As to claim 18, Ylonen discloses a computer system for establishing the secure transfer of a data packet between nodes in a workgroup over a public network, where the nodes are members of a VPN (Ylonen, col. 1, lines 23-26), the system comprising: a first node (Ylonen, Fig. 1, element 102; col. 1, lines 53-54); a second node (Ylonen, Fig. 1, element 106; col. 1, lines 58-59); a device detection mechanism; and a packet interception mechanism; where when a data packet is transferred from the first node to the second node and a device is detected at the second node, the data packet is intercepted and a packet header of the data packet is modified to facilitate the data transfer between the nodes (Ylonen, col. 1, lines 53-59).

Claim Rejections - 35 USC § 103

24. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

25. Claims 3, 7, and 9 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Muniyappa and further in view of Giniger et al. (U.S. 6,751,729).

26. As to claim 3, Muniyappa discloses a system for synchronizing the server and each of the connected nodes (Muniyappa, col. 5, lines 25-39). But Muniyappa does not expressly disclose detecting attribute revisions related to the nodes or the server. However, Giniger does teach a step of sensing attribute revisions relating to one of the connected nodes or the server (Giniger, col. 8, lines 53-65). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Muniyappa and Giniger in order to allow a VPN network to dynamically adapt to changes in the network topology with little manual intervention (Giniger, col. 6, lines 3-13).

27. As to claim 7, the combination of Muniyappa and Giniger (Muniyappa-Giniger) discloses the invention substantially including the method for establishing the system where each of the connected nodes automatically pull changes from the VPN server so as to update the configurational information stored at the node (Giniger, col. 8, lines 43-52).

28. As to claim 9, Muniyappa-Giniger discloses the invention substantially including where the system further comprises a datastore connected to the server (Giniger, col. 15, lines 8-15).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alicia Baturay whose telephone number is (571) 272-3981. The examiner can normally be reached at 7:30am - 5pm, Monday - Thursday, and every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain Alam can be reached on (571) 272-3978. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AB

HOSAIN ALAM
SUPERVISORY PATENT EXAMINER